УДК 004.056.52
DOI https://doi.org/10.32838/2663-5941/2019.4-1/21

Романюков М.Г.
Одеський національний політехнічний університет

ОРДИНАРНА МОДЕЛЬ ПРОЦЕСУ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ ВПЛИВУ НА МАТРИЦІ ЦІННОСТІ СУБ'ЄКТА В СИСТЕМІ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Аналізуючи поетапно процес розширення сфер застосування захисту інформації в Україні, можна стверджувати, що розширення сфер застосування захисту інформації відбувалось таким чином: від захисту інформації в технічних системах обробки інформації до захисту інформації в автоматизованих системах та комп'ютерних мережах, далі до інформаційної безпеки інформаційних ресурсів та важливих комунікацій, до інформаційної безпеки інформаційних технологій та критичних інфраструктур, далі до кібербезпеки кіберсередовища і в майбутньому до інтелектуальної безпеки інтелектуальних систем та соціально-психологічного захисту в рамках забезпечення національної безпеки. Можна спостерігати постійне вдосконалення засобів, технік і технологій захисту інформації в рамках їх застосування. Проступають контури парадигми забезпечення інтелектуальної безпеки, що включатиме сьогоднішні роботосистеми, штучний інтелект, Інтернет речей тощо. Характерною є важлива особливість розвитку систем інформаційної та кібербезпеки. На кожному з етапів попередні напрацювання не відкидаються, а навпаки, зберігаються і продовжують розвиватись. Засоби захисту протистоять певним загрозам і блокують їх. Якщо видалити ці засоби захисту, рано чи пізно старі загрози відродяться і можуть виникнути нові.

Так, виникає гостра необхідність дослідити найбільш вразливі елементи в сучасній структурі кібербезпеки держави, а саме матриці цінності суб'єкта впливу з боку протиборчої сторони, та побудувати ординарну модель впливу з боку протиборчої сторони, метою якої є досягнення як конструктивних, так і деструктивних цілей. Модель впливу будується з урахуванням показників практичного характеру, таких як кількість суб'єктів впливу, кількість впливів, необхідних для досягнення цілі впливів, а також імовірності того, що ці впливи досягнуть своєї мети. Математично модель впливу представляє собою аналітичну залежність між вказаними показниками. Застосування моделі дасть змогу вдосконалити процес планування інформаційних операцій та підвищити ефективність системи забезпечення кібербезпеки держави.

Ключові слова: *інформаційна операція, кібербезпека, вразливий елемент, суб'єкт впливу, матриця цінності суб'єкта, математична модель.*

Постановка проблеми. Стрімкий розвиток кібернетичного простору створив не лише очевидні переваги, але й низку проблем щодо захисту від кібернетичного впливу на військову, технологічну, політичну, інформаційну безпеку, суверенітет держави, а також на індивідуальну та суспільну свідомість. Тому цілком передбачувано виникає необхідність надійного контролю та постійного врегулювання відносин, що виникають у процесі життєдіяльності соціально-кібернетичної системи та невідкладного створення нових засобів забезпечення інформаційної та кібербезпеки [1, с. 16].

Україна разом з іншими країнами світу впевнено розв'язує завдання, що постають у процесі функціонування інформаційних систем та безпечної циркуляції як закритих, так і відкритих даних. Постійно зростаюча активність деструктивного когнітивного базису – інтернет-шпигунів, хакерів, звичайних користувачів, поєднання методів та інструментів збору інформації з різних джерел (у тому числі й закритих) і, як наслідок, відставання розвитку системи кібербезпеки призводять до активізації кіберзлочинності. Реалізація інформаційної та кібербезпеки в цьому випадку «буде полягати в реалізації функцій захисту інформаційних ресурсів та соціуму від проведення кібернетичних атак та спеціальних інформаційних операцій, що будуть спрямовані як на соціальну, так і на технічну частину соціотехнічної складової частини національної безпеки будь-якої держави» [2, с. 5].

Саме тому необхідною умовою створення безпечного інформаційного суспільства та організації боротьби зі зловмисниками є вирішення завдання з визначення найбільш вразливих елементів у системі кібербезпеки держави, побудувати відпо-

відні моделі впливу з боку протиборчої сторони. Своєчасність і актуальність тематики таких досліджень безсумнівна.

Аналіз останніх досліджень і публікацій. У сучасних наукових колах точаться різні дискусії щодо визначення поняття «кібербезпека» та «кібертероризм». Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. визначив термінологію, принципи та задачі кібербезпеки: «Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України в кіберпросторі».

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

У роботах [3, с. 119; 4, с. 133; 5, с. 50; 6, с. 2] проводяться дослідження та обґрунтування нового поняття «кібертероризм». До його змісту входить таке визначення: це застосування методів тероризму (створення в соціальній сфері обстановки страху, неспокою, пригніченості з метою прямого або непрямого впливу на прийняття будь-яких рішень) у кіберпросторі, мотивоване бажання до зміни політичних або ідеологічних змін, з огляду на те, що кібертероризм є транснаціональним і його вплив не залежить від географічного розташування терористів. Однак питання визначення найбільш вразливого елементу в системі кібербезпеки держави, а також побудови моделей впливу на нього з боку протиборчої сторони не вирішувалось.

Постановка завдання. Завданням статті є визначити найбільш вразливі елементи в системі кібербезпеки держави та побудувати ординарну модель процесу інформаційної операції впливу на матриці цінності суб'єктів із боку протиборчої сторони, метою якої є досягнення як конструктивних, так і деструктивних цілей, а також проаналізувати поведінку моделі та оцінити результати моделювання.

Виклад основного матеріалу дослідження. З психологічної точки зору, значна частина процесів людського життя відбувається безсвідомо, через настанови, стереотипи, культурні правила, побутові звички тощо. Це доведено експериментально [7, с. 13]. Тому, враховуючи сприяння зовнішнього середовища до алгоритмічної, операційної поведінки з урахуванням стереотипів, можна стверджувати, що люди легко переходять на автоматичний режим існування.

Так, виникає поняття «криптократія» – «не насильство, не переконання, а алгоритмізація, послідовне скорочення ступенів свободи і непомітне для людини перетворення особистих і групових інтересів у безумовну мотивацію досягнення зовнішніх для нього цілей» [8, с. 18]. Враховуючи вищевикладене, можна дійти висновку, що саме матриця цінностей кожного індивіда виступає суб'єктом впливу з боку зловмисника з метою реалізації (перепрограмування матриці цінностей) як конструктивних, так і деструктивних цілей.

У цьому разі під матрицею цінностей варто розуміти сукупність ціннісних понять (теоретичних, політичних, економічних, соціальних, естетичних, релігійних), які формують світобачення індивіда як особистості та визначають характер його поведінки в тій чи іншій ситуації, формуючи тим самим ядро особистості.

Результатом формування оцінки ймовірності перепрограмування матриці цінностей буде матриця, елементами якої є ймовірності дії окремих сеансів впливу.

Припустимо, що послідовність інформаційних впливів однакового спрямування змінює стан свідомості і підсвідомості суб'єкта пропорційно кількості дій. Нехай таких суб'єктів N. Через k позначимо число інформаційних впливів, необхідних для досягнення цілі, а через α – імовірність того, що вплив досягне своєї мети. Нехай $Y(k)$ – кількість суб'єктів (читачів, глядачів, слухачів, співбесідників), які змінили свою точку зору під дією k передач і почали інакше сприймати той чи інший термін або твердження.

Наша задача полягає в тому, щоб обґрунтувати аналітичну залежність Y від k. При цьому допускаємо, що всі дії мають однакову спрямованість і рівні за силою інформаційної дії.

Припустимо, що «у процесі першої інформаційної операції $Y(1) = \alpha N$ суб'єктів змінить свою точку зору щодо певного терміна, події або персонажа. Тоді залишиться $N - \alpha N = N(1 - \alpha)$ суб'єктів з особистою (не зміненою) матрицею цінностей. У процесі другої інформаційної операції $Y(2) = \alpha N(1 - \alpha)$ суб'єктів змінять свою точку зору щодо певного терміна, події або персонажа». Тоді залишиться [9, с. 30]:

$$Y(1) - Y(2) = N(1-\alpha) - \alpha N(1-\alpha) = \\ = N(1-\alpha)(1-\alpha) = N(1-\alpha)^2 \quad , \quad (1)$$

кількість суб'єктів з особистою (не зміненою) матрицею цінностей. У процесі третьої інформаційної операції $Y(3) = \alpha N(1-\alpha)^2$ суб'єктів змінять свою точку зору щодо певного терміна, події або персонажа. Тоді залишиться:

$$Y(1) - Y(2) - Y(3) = N(1-\alpha)^2 - \alpha N(1-\alpha)^2 = \\ = N(1-\alpha)^2(1-\alpha) = N(1-\alpha)^3 \quad , \quad (2)$$

кількість суб'єктів з особистою (не зміненою) матрицею цінностей. Міркуючи аналогічно, у процесі k - ї дії маємо:

$$Y(k) = \alpha N(1-\alpha)^{k-1}, \quad (3)$$

кількість суб'єктів, які будуть мати змінену матрицю цінностей (змінять свою точку зору щодо певного терміна, події або персонажа). Тоді залишиться:

$$Y(1) - Y(2) - Y(3) - ... - Y(k) = N(1-\alpha)^k, \quad (4)$$

суб'єктів з особистою (не зміненою) матрицею цінностей.

Однак у роботі [10, с. 241] вводиться поняття «інформаційна перевага», тобто змога забезпечити такий темп проведення інформаційної операції, який би переважав будь-який можливий темп жертви, що дало б змогу домінувати протягом усього часу її проведення.

З огляду на це визначення, кінцевим результатом, якого прагнутиме зловмисник, буде перепрограмування матриці цінностей усіх суб'єктів впливу з можливістю найскорішого завершення інформаційної операції.

Тому першочерговою необхідністю є визначення залежності кількості можливих інформаційних впливів k, необхідних для досягнення цілі зловмисника від імовірності α того, що ці впливи досягнуть своєї мети від повного перепрограмування заданої кількості суб'єктів N, на які здійснюється цей вплив. Нехай $Y(k) = 1$, тоді маємо:

$$1 = N(1-\alpha)^k, \quad (5)$$

$$N^{-1} = (1-\alpha)^k, \quad (6)$$

Прологаримуємо обидві частини рівності:

$$\lg N^{-1} = k \lg(1-\alpha), \quad (7)$$

звідки

$$k = -\frac{\lg N}{\lg(1-\alpha)} \quad , \quad (8)$$

Результати обчислень залежності кількості можливих інформаційних впливів k, необхідних для досягнення цілі зловмисника від імовірності α того, що ці впливи досягнуть своєї мети від повного перепрограмування заданої кількості суб'єктів N, на які здійснюється цей вплив, наведені у табл. 1.

Таблиця 1

Залежності кількості впливів k від імовірності α при кількості суб'єктів N

α	0,1	0,3	0,5	0,7	0,9	0,99
k для $N = 5 \cdot 10^4$	102	30	16	9	5	2
k для $N = 1 \cdot 10^5$	109	32	17	10	5	2
k для $N = 2 \cdot 10^5$	115	34	18	11	5	2
k для $N = 4 \cdot 10^5$	122	36	19	11	6	2
k для $N = 6 \cdot 10^5$	126	37	19	11	6	2
k для $N = 8 \cdot 10^5$	129	38	19	11	6	2
k для $N = 1 \cdot 10^6$	131	39	20	11	6	2

Представимо результати, наведені в табл. 1, у вигляді графічної залежності (рис. 1) імовірності α того, що впливи зловмисника на матриці цінностей суб'єктів впливу досягнуть своєї мети від повного перепрограмування заданої кількості суб'єктів N, за різної кількості можливих інформаційних впливів, необхідних для досягнення цілі зловмисника k.

Аналіз дослідження показує, що за ймовірності того, що інформаційні впливи з боку протиборчої сторони досягнуть своєї мети $\alpha \le 0,3$, зловмисникові необхідно суттєво збільшувати кількість впливів k зі зростанням кількості охоплюваних суб'єктів (кількості населення) впливу N. При значеннях імовірності того, що інформаційні впливи з боку протиборчої сторони досягнуть своєї мети $\alpha \ge 0,7$, кількість впливів k зі сторони зловмисника може практично не змінюватись зі зростанням кількості охоплюваних суб'єктів (кількості населення) впливу N.

Важливим параметром повного перепрограмування суб'єктів впливу є визначення залежності імовірності α того, що впливи на матрицю цінностей суб'єктів впливу зі сторони зловмисника досягнуть своєї мети, від заданої кількості суб'єктів N, що охоплені впливом, при різній кількості впливів k. Проведемо відповідні розрахунки. Прологарифмуємо обидві частини рівності (5) та виконаємо необхідну умову $Y(k) = 1$, отже, маємо:

$$\lg(1-\alpha) = -\frac{\lg N}{k}; \quad 1-\alpha = 10^{\frac{-\lg N}{k}}, \quad (9)$$

звідки

$$\alpha = 1 - 10^{\frac{-\lg N}{k}}, \quad (10)$$

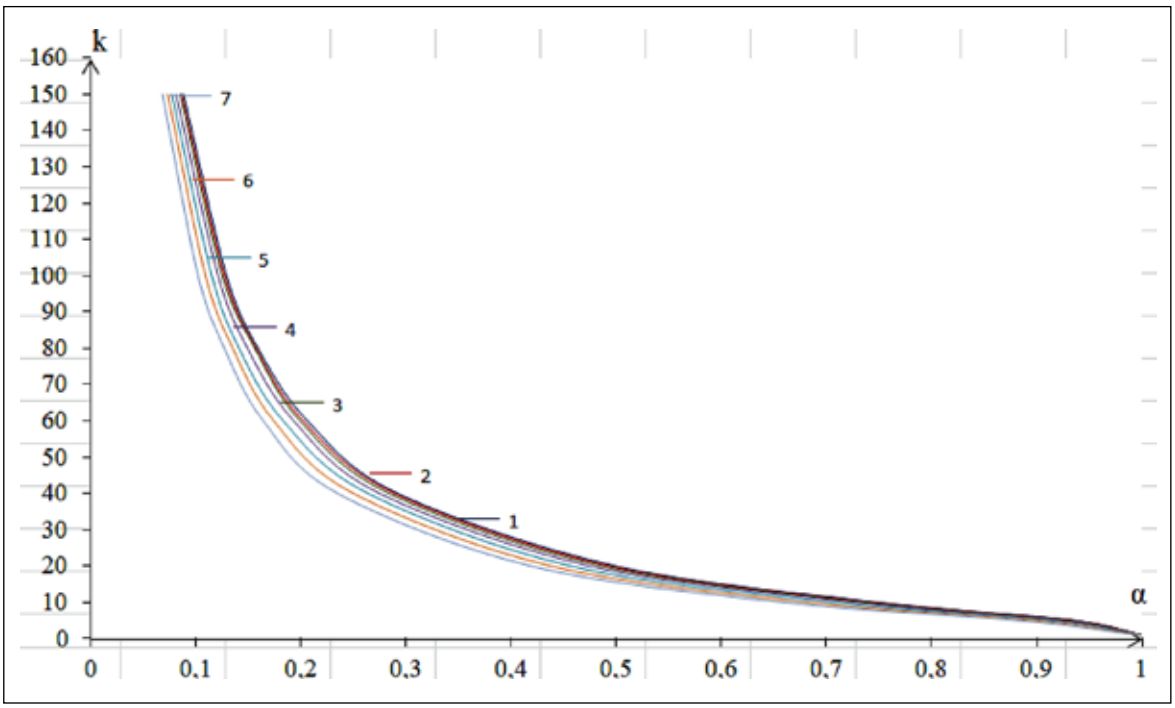

Рис. 1. Графічні залежності кількості впливів k від імовірності α при кількості суб'єктів N (1 – $N = 1 \cdot 10^6$; 2 – $N = 8 \cdot 10^5$; 3 – $N = 6 \cdot 10^5$; 4 – $N = 4 \cdot 10^5$; 5 – $N = 2 \cdot 10^5$; 6 – $N = 1 \cdot 10^5$; 7 – $N = 5 \cdot 10^4$)

Таблиця 2

Залежності імовірності α від заданої кількості суб'єктів N, що охоплені впливом, при різній кількості впливів k

N	$5 \cdot 10^4$	$1 \cdot 10^5$	$2 \cdot 10^5$	$4 \cdot 10^5$	$6 \cdot 10^5$	$8 \cdot 10^5$	$1 \cdot 10^6$
α для $k = 1$	0,999980	0,999990	0,999995	0,999997	0,999998	0,999998	0,99999
α для $k = 5$	0,885	0,900	0,9129	0,924	0,930	0,934	0,937
α для $k = 10$	0,660	0,682	0,705	0,725	0,736	0,743	0,749
α для $k = 20$	0,419	0,438	0,457	0,475	0,486	0,493	0,499
α для $k = 40$	0,235	0,250	0,264	0,275	0,284	0,289	0,292
α для $k = 60$	0,164	0,174	0,183	0,193	0,199	0,202	0,206
α для $k = 80$	0,127	0,135	0,141	0,149	0,156	0,157	0,159
α для $k = 100$	0,102	0,109	0,115	0,121	0,125	0,127	0,129
α для $k = 150$	0,068	0,073	0,077	0,081	0,085	0,086	0,088

Результати обчислень залежності імовірності α того, що впливи на матрицю цінностей із повним її перепрограмуванням досягнуть своєї мети, від заданої кількості суб'єктів N, що охоплені впливом, при різній кількості впливів k, наведені у табл. 2.

Представимо результати наведені у табл. 2 у вигляді графічної залежності (рис. 2) ймовірності α того, що впливи на матрицю цінностей із повним її перепрограмуванням досягнуть своєї мети від заданої кількості суб'єктів N, що охоплені впливом, при різній кількості впливів k.

Аналіз дослідження показує, що для кожного значення кількості суб'єктів перепрограмування N, метою зловмисника щодо яких є повне перепрограмування матриць цінностей, імовірності α того, що впливи на матрицю цінностей із повним її перепрограмуванням досягнуть своєї мети, може зменшуватись зі збільшенням кількості впливів k.

Таким чином, зростання імовірності α того, що впливи на матрицю цінностей з повним її перепрограмуванням досягнуть своєї мети, зі

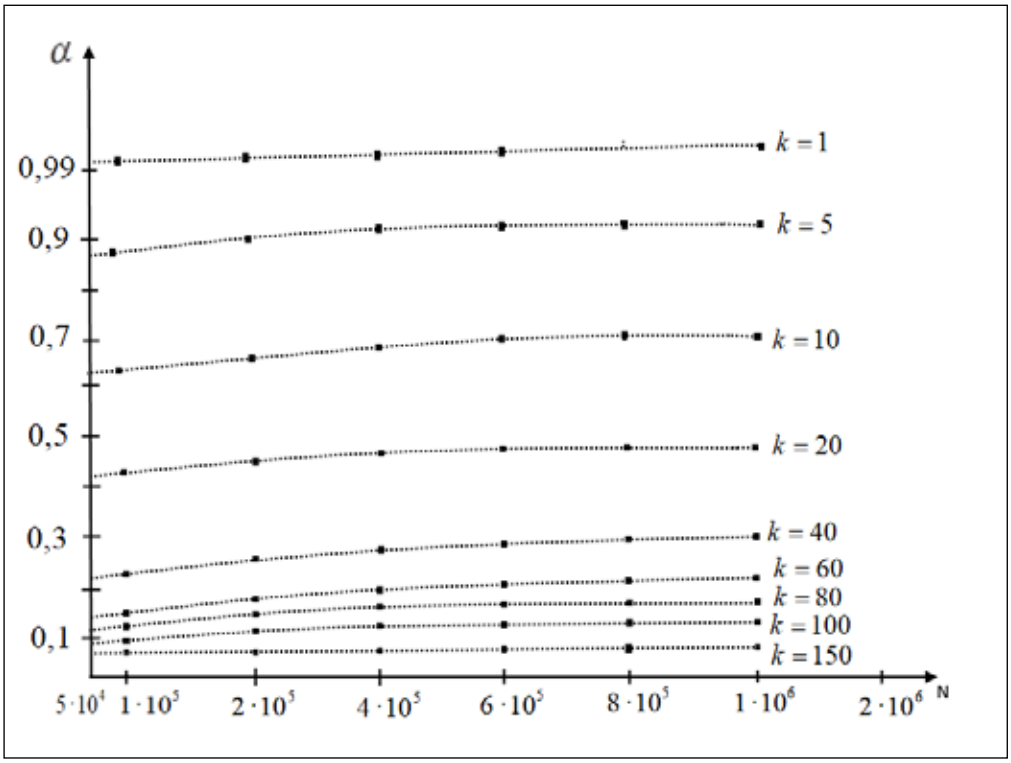

Рис. 2. Графічні залежності імовірності α від заданої кількості суб'єктів N, що охоплені впливом, при різній кількості впливів k

зростанням кількості населення (суб'єктів перепрограмування) N при відповідній кількості впливів k свідчить про те, що для повного перепрограмування суб'єктів впливу з кількістю N, зловмисник буде намагатися досягти своєї мети шляхом збільшення імовірності α, здійснюючи задану кількість впливів k, а також зі збільшенням кількості суб'єктів впливу збільшувати імовірність їхнього перепрограмування.

Висновки. У цій роботі вирішено важливе нині завдання, що постає перед фахівцями інформаційної безпеки та кібербезпеки. Визначено матрицю цінностей кожного індивіда як найбільш вразливий елемент системи кібербезпеки. Вперше побудовано ординарні моделі процесу інформаційної операції впливу на матрицю цінностей із боку протиборчої сторони, з огляду на показники практичного характеру: кількість суб'єктів впливу, кількості впливів, необхідних для досягнення цілі, а також імовірності того, що ці впливи досягнуть своєї мети. Застосування моделі дасть змогу удосконалити процес планування інформаційних операцій та підвищити ефективність системи забезпечення кібербезпеки держави.

Напрямом подальших досліджень є створення методів та засобів оцінки ефективності системи захисту свідомості і підсвідомості суб'єктів від деструктивних інформаційних впливів.

Список літератури:

1. Грищук Р.В. Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни. *Кібербезпека в Україні: правові та організаційні питання :* матеріали всеукр. наук.-практ. конф. Одеса, 21 жовтня 2016 р. Одеса, 2016. С. 16–17.

2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезбека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

3. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. Т. 19. № 2. С. 118−129.

4. Харченко В.П., Чеботаренко Ю.Б., Корченко О.Г., Паціра Є.В., Гнатюк С.О. Кибертерроризм на авиационном транспорте. *Проблеми інформатизації та управління.* Збірник наук. пр. НАУ. 2009. № 4 (28). С. 131−140.

5. Довгань О.Д., Хлань В.Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави*. 2011. № 3 (7). С. 49−53.

6. Mayssa Zerzri The Threat of Cyber Terrorism and Recommendations for Countermeasures. URL: https://www.caplmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf?m=1510830733& (дата звернення: 12.07.2019).

7. Аллахвердов В.М. Методологическое путешествие по океану бессознательного к таинственному острову сознания. Санкт-Петербург : Речь, 2003. 368 с.

8. Ларина Е.С. Понимание алгоритмических обществ: гибридный интеллект и его зомби. *Свободная мысль.* 2017. № 5. С. 5−26.

9. Расторгуев С.П., Литвиненко М.В. Информационные операции в сети Интернет. Москва : АНО ЦСОиП, 2014. 128 с.

10. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Санкт-Петербург : Наукоемкие технологии, 2017. 549 с.

Romanyukov M.G. ORDINARY MODEL OF THE PROCESS OF INFORMATION OPERATION OF THE INFLUENCE ON THE MATRIX OF THE SUBJECT VALUE IN THE SYSTEM OF THE UKRAINE'S CIBERDS OF THE STATE

Analyzing the phased process of expanding the scope of information protection in Ukraine, it can be argued that the expansion of the scope of protection of information was as follows: from the protection of information in technical information processing systems; to protect information in automated systems and computer networks; further to the information security of information resources and important communications; to the information security of information technologies and critical infrastructures, further to the cyber security of cybernetics and, in the future, to the intellectual security of intellectual systems and socio-psychological protection within the framework of national security. You can observe the constant improvement of the means, techniques and technologies of information protection within the framework of their application. The contours of the next paradigm of providing intellectual security that will include today's robotsystems, artificial intelligence, Internet stuff, and the like. A characteristic feature of the development of information and cyber security systems is characteristic. At each stage, previous work is not discarded, but rather stored and continue to develop. Means of protection confront certain threats and block them. If you remove these security tools sooner or later, the old threats will resurrect and new ones may emerge.

Thus, there is an urgent need to investigate the most vulnerable elements in the modern structure of the cyber security of the state, namely the matrix of the value of the subject of influence from the side of the opposing side, and to build an ordinary model of influence from the side of the opposing side, whose purpose is to achieve both constructive and destructive goals. The impact model is based on practical indicators, such as the number of actors of influence, the number of impacts needed to achieve the goal of impacts, and the likelihood that these impacts will achieve their goal. Mathematically, the model of influence is an analytical relationship between the indicated indicators. Application of the model will enable to improve the process of planning of information operations and increase the efficiency of the system of ensuring cybersecurity of the state.

Key words: *information operation, cybersecurity, the most vulnerable element, subject of influence of the matrix of the value of the subject, mathematical model.*